REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN

DOC TYPE: New Work Item Proposal (NP)

TITLE: A New Work Item Proposal on "Suppliers' declaration of conformity for IT security products"

SOURCE: 11th SC 27 plenary meeting

DATE: 1999-10-12

PROJECT: NP

STATUS: In accordance with resolution 26 (SC 27 N 2466) of the 11th SC 27 plenary meeting in Columbia, MD, USA, October 11 – 13, 1999, this document has been sent to the JTC 1 Secretariat for a 3-month NP letter ballot. It is being circulated within SC 27 for information.

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
W. Fumy, SC 27 Chairman
M. De Soete, T. Humphreys, M. Ohlin, WG-Conveners

MEDIUM: Server

NO. OF PAGES: 5

Date of presentation of proposal: 1999-10-12	Proposer: ISO/IEC JTC 1/SC 27
Secretariat: ISO/IEC JTC1/SC 27 National Body: DIN, Germany	**ISO/IEC JTC 1 N**

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of a proposal - to be completed by the proposer Guidelines for proposing and justifying a new work item are given in ISO Guide 2

Title: Suppliers' declaration of conformity for IT security products
Scope: The standard defines the content and structure of a Suppliers' Declaration of conformity for IT Security Products
Purpose and justification – See attached Purpose and Justification

Programme of work

If the proposed new work item is approved , which of the following document(s) is (are) expected to be developed?

__X

osej T939ustifica956ndard moG/F4n a Tdted xpec   ) expected to be - 3o b3915 1 N

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A Business Requirement		
A.1 Market Requirement	Essential _**X**__ Desirable ___ Supportive ___	
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive _**X**__ Not Relevant ___	
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No_**X**__	
B.2 Commitment to other organization	Yes ___ No_**X**__	
B.3 Other Source of standards	Yes ___ No_**X**__	
C. Technical Status		
C.1 Mature Technology	Yes _**X**__ No___	
C.2 Prospective Technology	Yes ___ No_**X**__	
C.3 Models/Tools	Yes ___ No_**X**__	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes _**X**__ No___	
D.2 Interoperability	Yes ___ No_**X**__	
E. Other Justification		

ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - "Information Technology"
SC 27 - "Security Techniques"
WG 3 - "Security Evaluation Criteria"

TITLE: Suppliers' Declaration of Conformity for IT Products

SOURCE: Johannes Appel, Germany

DATE: 1999-10-08

PROJECT:

STATUS: This document is being submitted for consideration at the 19 th SC 27/WG 3 meeting
            in Columbia, MD, U.S.A., October 4 - 8, 1999.

Proposed New Work Item

A new standard was proposed at the ISO/IEC SC27 WG3 meeting in Columbia, MD, U.S.A., October 4 - 8, 1999. The purpose of the standard is to formalise the Manufacturers commitment to his product with a Suppliers' Declaration of Conformity (SDoC). The use of SDoC is an accepted method in the international community to confirm the compliance of applied standards. However, as of today it in not used in the field of IT security. The intent of this standard is to close this gap. Therefore, this standard will be a major contribution to increase the transparency and comparability for the manufacturers, vendors, and end users in selecting trustworthy products.

It should describe the required structure and content of the SDoC for IT security products. The criteria and/or standards used for the evaluation of the security function and the assurance method applied during the development, production, and shipment of IT product should be stated in a prescribed manner.

The development of the SDOC content should consider the following:
- Gives the name and address of the supplier who issued the declaration
- Describes the IT security equipment and/or software in terms of name, type and model number
- Bears the place and date when the declaration was issued
- States the number, titles, and date of the applied evaluation criteria, standards, design and assurance methodology and any other reference, if applicable, like
    - EU directives
    - company intern measures which ensure the compliance of the product with the required level of security
    - other supporting document
- Gives the evaluation report reference number
- In case the evaluation was carried out by an independent test house, gives additionally the name and address of the test laboratory which issued an evaluation report and/or certificate including a number and issue date
- Carries a signature of the supplier or his authorised representative.

The supplier confirms the compliance of a product with the applied evaluation criteria by issuing a SDoC in the same language as the operating instruction.
He keeps a file with the exact technical specification, construction data, test- and evaluation plan and results or evaluation report and certificate. The SDoC is included with every product shipped, and part of the operating instruction or any other customer documents. The manufacturer or supplier will supply the SDoC to its consumer on request.

The content of the SDoC can be used for any form of IT security evaluation.